This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS

1. (Currently Amended) A method for verifying that data received by a receiver have been sent by a transmitter authorized by a trusted third party, the transmitter and the receiver being connected to a digital network, wherein an identifier is associated with the data sent by the transmitter, ~~and in that~~ the method ~~comprises the steps consisting,~~ for the receiver comprising: ~~, in:~~

(a) generating a random number;

(b) broadcasting said random number and said identifier over the network;

(c) receiving from the transmitter a response computed by applying a first function to said random number and to said identifier;

(d) verifying the received response by applying a second function to the received response, to said random number and to said identifier;

the first function having previously been delivered to the transmitter by the trusted third party and the second function being a function for verifying the result of the first function, previously delivered by the trusted third party to the receiver.

2. (Previously Presented) The method as claimed in claim 1, in which the step (b) is replaced by a step consisting in sending said random number to the transmitter.

3. (Cancelled)

4. (Previously Presented) The method as claimed in claim 1, wherein the receiver inhibits access to said data if the response received in the step (c) is not correct or if no response is received after the expiry of a predetermined time starting from the transmission of the random number.

5. (Currently Amended) A method for proving that data sent to a receiver have been transmitted by a transmitter authorized by a trusted third party, the transmitter and the receiver being connected to a digital network, wherein an identifier is associated with the data sent by the transmitter, ~~and in that~~ the method ~~comprises the steps consisting,~~ for the transmitter comprising: ~~in:~~

(a) receiving a random number from the receiver;

(b) computing a response by applying a first function to said random number and to said identifier;

(c) sending said response to the receiver;

said response being ~~likely to be~~ verified by the receiver by applying a second function to the received response, to said random number and to said identifier;

the first function having previously been delivered to the transmitter by the trusted third party and the second function ~~(H)~~ being a function for verifying the result of the first function, previously delivered by the trusted third party to the receiver.

6. (Currently Amended) The method as claimed in claim 5, in which ~~the transmitter also receives in the step (a) said identifier associated with the data received by the receiver and in which the~~ steps (b) and (c) are not carried out unless said identifier received in the step (a) corresponds to the identifier associated with the data that the transmitter has just sent.

7. (Previously Presented) The method as claimed in claim 1, wherein the identifier associated with the data sent by the transmitter is a random number generated by the initial transmitter of the data in the network and attached to said data by the initial transmitter.

8. (Previously Presented) The method as claimed in claim 1, wherein the first function is a public function using a secret key.

9. (Currently Amended) The method as claimed in claim 8, wherein the second function is a boolean function and further comprising:

computing an expected response by applying to said random number and to said identifier the first function with the secret key and

comparing the expected response with the response received in order to deliver:

- a "0" value if the expected and received responses are different and
- a "1" value if the expected and received responses are equal.

10. (Previously Presented) The method as claimed in claim 1, wherein the first function is a secret function.

11. (Currently Amended) The method as claimed in claim 10, wherein the second function is a boolean function and further comprising:

computing an expected response by applying the first function to said random number and to said identifier and

comparing the expected response with the received response in order to deliver:

- a "0" value if the expected and received responses are different and
- a "1" value if the expected and received responses are equal.

12. (Previously Presented) The method as claimed in claim 1, wherein the first function is a public function for signature generation with the aid of a private key.

13. (Previously Presented) The method as claimed in claim 12, wherein the second function is a public function for signature verification with the aid of a public key corresponding to the private key used by the first function.